

**Notice of Allowability**

Application No.

09/759,443

Applicant(s)

CORELLA, FRANCISCO

Examiner

Christian La.Forgia

Art Unit

2131

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 27 June 2005.
2. ☒ The allowed claim(s) is/are 1-14, 16-34, 36, 37, 42-44 and 46-59.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All    b) ☐ Some\*    c) ☐ None    of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.


Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
  - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
    - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
  - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08),  
Paper No./Mail Date 7/1/05, 8/22/05
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413),  
Paper No./Mail Date \_\_\_\_\_.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_.

  
AMY SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2131

### EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Patrick Billig on 16 September 2005.

The application has been amended as follows:

Claim 21: A method for managing the validity status of a subject's public key comprising:

generating, with an off-line registration authority, a first public key serial number (PKVN) having a high probability of being different from all previously generated PKVNs previously generated by the registration authority;

issuing, with the off-line registration authority, to a subject a first unsigned public key validation certificate (unsigned PKVC) that binds a public key of the subject to the first PKVN;

maintaining, with the off-line registration authority, a certificate database of unsigned PKVCs in which the first unsigned PKVC is stored;

issuing, with an on-line credentials server, to the subject a disposable public key validation certificate (disposable PKVC), that binds the public key of the subject from the first unsigned PKVC to the first PKVN from the first unsigned PKVC; and

maintaining, with the on-line credentials server, a table that contains entries corresponding to valid unsigned PKVCs stored in the certificate database.

Art Unit: 2131

Claim 37: A public key infrastructure (PKI) comprising:

a subject; and

a first public key validation agent (PKVA) including:

an off-line registration authority configured to generate a first public key serial number (PKVN) having a high probability of being different from all other PKVNs previously generated by the registration authority, to issue a first unsigned public key validation certificate (unsigned PKVC) off-line to a subject that binds a public key of the subject to the first PKVN, and to maintain a certificate database of unsigned PKVCs in which it stores the first unsigned PKVC; and

an on-line credentials server configured to issue a disposable public key validation certificate (disposable PKVC) on-line to the subject, the disposable PKVC binds the public key of the subject from the first unsigned PKVC to the first PKVN from the first unsigned PKVC, wherein the credentials server is configured to maintain a table that contains entries corresponding to a valid unsigned PKVCs stored in the certificate database configured to maintain a record representing the status of validity of the subject's public key, the record has a high probability of being different from all other records of the first PKVA or of any other PKVA; and

a verifier configured to respond to an authentication of the subject, wherein the authentication includes ascertaining the validity of the subject's public key according to the ~~record of the first PKVA~~ table maintained by the credentials server.

Art Unit: 2131

Claims 38-41: (Cancelled)

Claim 42: The PKVA of claim [[41]] 37 wherein the first PKVA is configured to respond to a request for invalidating the subject's public key, the first PKVA's response includes abstaining from issuing the ~~second certificate~~ disposable PKVC.

Claim 43: The PKI of claim [[41]] 37 wherein the PKVA is configured to require the representation of the issued first ~~issued certificate~~ unsigned PKVC from the subject in order to issue the ~~second certificate~~ disposable PKVC.

Claim 44: The PKI of claim [[41]] 37 wherein the ~~second certificate~~ disposable PKVC is a signed certificate.

Claim 45: (Cancelled)

Claim 46: The PKI of claim [[45]] 37 wherein the disposable ~~certificate~~ PKVC is configured to expire after a selected passage of time.

Claim 47: The PKI of claim [[45]] 37 wherein the disposable ~~certificate~~ PKVC is configured to expire on a selected date/time.

Art Unit: 2131

Claim 48: The PKI of claim 37 wherein the ~~maintained record is~~ entries in the table maintained by the credentials server are keyed by a cryptographic hash.

Claim 53: The PKVA of claim 49 wherein the responding includes altering the ~~maintained record~~ an entry in the table maintained by the credentials server.

Claim 55: The PKVA of claim 53 wherein the altering includes removing the ~~maintained record~~ the entry in the table maintained by the credentials server.

Claim 56: The PKVA of claim 49 wherein the responding includes altering accessibility to the ~~maintained record~~ an entry in the table maintained by the credentials server.

Claim 57: The PKI of claim 37 ~~further comprising a~~ wherein the registration authority is configured to authenticate the subject, the authentication comprises verifying that at least one purported identity attribute of the subject in fact applies to the subject.

Claim 58: The PKI of claim 57 wherein the registration authority is configured to respond to an assertion of the validity of the subject's public key, the assertion is based on ~~the record~~ an entry in the table maintained by the ~~first PKVA~~ credentials server.

***Terminal Disclaimer***

The terminal disclaimer filed on 27 June 2005 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of U.S. Patent No. 6,763,459 has been reviewed and is accepted. The terminal disclaimer has been recorded.

***Information Disclosure Statement***

The information disclosure statement (IDS) submitted on 01 July 2005 is in compliance with the provisions of 37 CFR 1.97, and is being considered by the examiner.

The information disclosure statement (IDS) submitted on 22 August 2005 is in compliance with the provisions of 37 CFR 1.97, and is being considered by the examiner.

***Response to Arguments***

Applicant's arguments, see the second paragraph of page 12, filed 27 June 2005, with respect to claims 1, 21, and currently amended 37 have been fully considered and are persuasive. The rejection of claims 1-14, 16-34, 36, 37, 42-44, and 46-59 has been withdrawn.

***Allowable Subject Matter***

Claims 1-14, 16-34, 36, 37, 42-44, and 46-59 are allowed.

The following is an examiner's statement of reasons for allowance:

The Examiner agrees with the Applicant's arguments that the prior art does not disclose issues off-line an disposable unsigned public key validation certificate to a subject that binds the public key of the subject to the first public key validation number and that the certificate database cannot be both the certificate database and the certificate table.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue

Art Unit: 2131

fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

*Conclusion*


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia  
Patent Examiner  
Art Unit 2131

clf

  
AYAZ SHEIKH  
SUPERVISORY PROJECT EXAMINER  
TECHNOLOGY CENTER 2100